UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/943,893	08/30/2001	Shinako Matsuyama	09792909-5132	2067

26263 7590 08/28/2003

SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO, IL 60606-1080

EXAMINER
PAIK, STEVE S

ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 08/28/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/943,893	MATSUYAMA ET AL.	
	Examiner	Art Unit	
	Steven S. Paik	2876	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 June 2003* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Amendment

1. Receipt is acknowledged of the Amendment filed June 9, 2003. The Applicant amended claims 1-28 and replaced the Abstract. The arguments has been fully considered.

Claim Objections

2. Claims 1 and 2 are objected to because of the following informalities: the limitation, "the person authentication certificate" in lines 5, 8, and 11 appears lacking the antecedent basis. The examiner respectfully suggests replacing it by -- the electronic person authentication certificate – to overcome the objection. Dependent claims also contain aforementioned issue of lacking the antecedent basis. Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 2, 4, 5, 11-15, 17, 18, 24, and 28 are rejected under 35 U.S.C. 102(e) as being anticipated by Dulude et al. (US 6,310,966).

Re claims 1, 4, and 5, Dulude et al. disclose a person authentication system (Figs. 3-5, the Registration System 24, Transmitting section 40, and Receiving section 42) for executing personal authentication by comparing a template with sampling information, the template being

person authentication data (biometric data 20 in Fig. 2), and the sampling information (col. 5, ll. 52-54) being input (44) by a user (first user), the person authentication system comprising:

a person authentication authority (Biometric Certificate Generator 32 in Registration Authority 34 of Fig. 2) for issuing an electronic person authentication certificate (biometric certificate 16) including the template (20);

a person authentication execution entity (Biometric certificate extractor 64, second classifier 84 in Receiving section 42) for obtaining the certificate including the template from the person authentication certificate (biometric certificate extractor accesses a corresponding biometric certificate 16 stored in the memory 66) issued by said person authentication authority (34) and executing person authentication on the basis of the obtained template (col. 6, ll. 58-65);

wherein the person authenticate certificate (16) issued by said person authentication authority (Biometric Certificate Generator 32 in Registration Authority 34 of Fig. 2) stores usage restriction information (validity period; col. 2, ll. 8-9) which includes at least either a certificate expiration date or usage number limit; and

said person authentication entity (Biometric certificate extractor 64, second classifier 84 in Receiving section 42) checks the validity of the person authentication certificate (16) on the basis of the certificate expiration date (Biometric certificate extractor 64 accesses biometric certificate 16 stored in the memory or database 66. The biometric certificate includes a data filed for validity period.) or the certificate usage number limit when the person authentication is executed on the basis of the person authentication certificate (col. 2, ll. 5-17).

Re claim 2, Dulude et al. disclose the person authentication system (Figs. 3-5, the Registration System 24, Transmitting section 40, and Receiving section 42) as recited in rejected

claim 1 stated above, where said person authentication execution entity (Biometric certificate extractor 64, second classifier 84 in Receiving section 42) checks the validity of the person authentication certificate (16) on the basis of the certificate expiration date or certificate usage number limit (validity period) in person authentication on the basis of the person authentication certificate, and then executes the person authentication by comparing the template (20), stored in the person authentication certificate (16), with sampling information input (46; col. 5, ll. 52-54) by the user (first user) on the condition that the validity of the person authentication certificate has been confirmed on the basis of the certificate expiration date or the certificate usage number limit (validity period). Since the biometric data is from indicia based on the physical characteristics of the individuals including, not limited to, generic composition, facial characteristics, etc. As times goes, the physical characteristics inherently change. Thus, it is necessary to limit a validity of such biometric data for the purpose of providing authentication process with close to zero error rate.

Re claims 11 and 13, Dulude et al. disclose the person authentication system (Figs. 3-5, the Registration System 24, Transmitting section 40, and Receiving section 42) as recited in rejected claim 1 stated above, wherein said person authentication authority and said person authentication executing entity execute mutual authentication, when data communication is performed therebetween, a data transmitter (48) puts a digital signature (22) on transmitted data, and a data receiver verifies the digital signature (col. 7, ll. 26-44).

Re claim 12, Dulude et al. disclose the person authentication system (Figs. 3-5, the Registration System 24, Transmitting section 40, and Receiving section 42) as recited in rejected claim 1 stated above, wherein the template (20) is at least one of personal biotic information,

personal non-biotic information, and a password, wherein the personal biotic information (first category) is selected fro at least one of the group consisting of fingerprint information, retina pattern information, iris pattern information, voice print information (col. 4, ll. 26-32), and handwriting information (col. 2, ll. 54-60), and wherein the personal nonbiotic information (second category) is selected from at least one of the first group consisting of seal information, passport information, driver's license information, and card information (col. 2, ll. 61-67 and col. 3, ll. 1-2).

Re claims 14, 17, and 18, Dulude et al. disclose a person authentication method (Figs. 3-5, the Registration System 24, Transmitting section 40, and Receiving section 42) for executing personal authentication by comparing a template with sampling information, the template being person authentication data (biometric data 20 in Fig. 2), and the sampling information (col. 5, ll. 52-54) being input (44) by a user (first user), the person authentication method comprising:

causing a person authentication authority (Biometric Certificate Generator 32 in Registration Authority 34 of Fig. 2) for issuing an electronic person authentication certificate (biometric certificate 16) including the template (20);

causing a person authentication execution entity (Biometric certificate extractor 64, second classifier 84 in Receiving section 42) to obtain the certificate including the template from the person authentication certificate (biometric certificate extractor accesses a corresponding biometric certificate 16 stored in the memory 66) issued by said person authentication authority (34) and executing person authentication on the basis of the obtained template (col. 6, ll. 58-65);

storing usage restriction information (validity period; col. 2, ll. 8-9) which includes at least either a certificate expiration date or usage number limit; and

causing the person authentication entity (Biometric certificate extractor 64, second classifier 84 in Receiving section 42) checks the validity of the person authentication certificate (16) on the basis of the certificate expiration date (Biometric certificate extractor 64 accesses biometric certificate 16 stored in the memory or database 66. The biometric certificate includes a data filed for validity period.) or the certificate usage number limit when the person authentication is executed on the basis of the person authentication certificate (col. 2, ll. 5-17).

Re claim 15, Dulude et al. disclose the person authentication method (Figs. 3-5, the Registration System 24, Transmitting section 40, and Receiving section 42) as recited in rejected claim 14 stated above, wherein the person authentication execution entity (Biometric certificate extractor 64, second classifier 84 in Receiving section 42) checks the validity of the person authentication certificate (16) on the basis of the certificate expiration date or certificate usage number limit (validity period) in person authentication on the basis of the person authentication certificate, and then executes the person authentication by comparing the template (20), stored in the person authentication certificate (16), with sampling information input (46; col. 5, ll. 52-54) by the user (first user) on the condition that the validity of the person authentication certificate has been confirmed on the basis of the certificate expiration date or the certificate usage number limit (validity period). Since the biometric data is from indicia based on the physical characteristics of the individuals including, not limited to, generic composition, facial characteristics, etc. As times goes, the physical characteristics inherently change. Thus, it is necessary to limit a validity of such biometric data for the purpose of providing authentication process with close to zero error rate.

Re claim 24, Dulude et al. disclose the person authentication method (Figs. 3-5, the Registration System 24, Transmitting section 40, and Receiving section 42) as recited in rejected claim 14 stated above, wherein said person authentication authority and said person authentication executing entity execute mutual authentication, when data communication is performed therebetween, a data transmitter (48) puts a digital signature (22) on transmitted data, and a data receiver verifies the digital signature (col. 7, ll. 26-44).

Re claim 28, Dulude et al. disclose a program providing medium for providing a computer program which executes (Figs. 3-5, the Registration System 24, Transmitting section 40, and Receiving section 42) for) person authentication on the compute program by comparing a template (20) stored in a person authenticate certificate (16) with sampling information, the template being person authentication data (biometric data 20 in Fig. 2), and the sampling information (col. 5, ll. 52-54) being input (44) by a user (first user), the computer program comprising:

a step of confirming whether usage restriction information (validity period) , which includes either a certificate expiration date, a certificate usage number limit, or a template expiration date, is stored in the person authenticate certificate issued by a person authentication authority (34);

a step of checking the validity of the person authentication certificate on the basis of the certificate expiration date, the certificate usage number limit, or a template expiration date in the person authentication on the basis of the person authenticate certificate (data stored in biometric database or smart card memory 66 are accessed via biometric certificate extractor 64 to verify the validity of the biometric data in the person authentication certificate.)

a step of executing the person authentication by comparing the template (by second classifier 84), which is stored in the person authenticate certificate, with the sampling information (transaction biometric data 46) input by user on a condition that the validity of the person authentication certificate has been confirmed on the basis of the certificate expiration date, certificate usage number limit, or the template expiration date.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 3, 16, 25, 26, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dulude et al. (US 6,310,966) in view of Epstein (US 6,601,046).

Re claims 3, 16, 25, 26 and 27, Dulude et al. disclose a person authentication system including all of the claimed features of the invention with the exception of storing a usage count in a memory of the person authentication executing device.

Although Dulude et al. disclose the biometric system comprising a biometric certificate including validity period data, the reference fails to disclose or fairly suggest a usage counter.

Epstein discloses a system having a usage-limit function to protect the authenticity of copy-protected material, watermarking, ticketing, and the like. The system verifies the authenticity of the parameters and provides access to a copy-protected material only within the associated usage-limit of the material (Abstract). The usage-limit prevents the copy-protected

material from being regenerated without a proper authentication process. Therefore, unauthorized usage of the copy-protected material is tightly controlled.

In view of Epstein, it would have been obvious to an artisan of ordinary skill in the art at the time the invention was made to further incorporate the teachings of verifying the expiry of usability of the copy-protected material in addition to the biometric authentication system of Dulude et al. due to the fact that an access to play the copy-protected material is more accurately and selectively given and the number of accessing the copy is limited to a predetermined number for the purpose controlling the number of access given to a particular material. Furthermore, such modification of employing the concept of limiting the usage of a copy-protected material, as taught by Epstein, to the teachings of Dulude et al. would have been an obvious matter of design variation, well within the ordinary skill in the art, and therefore an obvious expedient.

7. Claims 6-10 and 19-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dulude et al. (US 6,310,966) in view of Ohtsuki et al. (US 5,831,547).

The teachings of Dulude et al. have been discussed above. Dulude et al. disclose a person authentication system including all of the claimed features of the invention with the exception of specifically disclosing means for giving notice of approaching expiration date.

Ohtsuki et al. discloses a processor 202 reading the expiration date and the present date from the time and date clock 206. The processor compares the expiration data to the present date. If the time remaining until the expiration date is smaller than a predetermined number, the processor provides a signal to notify the user of the card (col. 6, lines 12-22). It is suggested that the expiration data can be modified according to the user's preset data (col. 6, ll. 53-57).

Therefore, it would have been obvious at the time the invention was made to a person having of ordinary skill in the art to have added means for keeping the current time and comparing it to an expiration date, as taught by Ohtsuki et al., into the teachings of Dulude et al. for the purpose of informing the user of remaining time until the expiration date and allowing opportunity to modify the time sensitive information according to the needs of a user.

Response to Arguments

8. Applicant's arguments with respect to claims 1-28 have been considered but are moot in view of the new ground(s) of rejection. The newly cited reference Dulude et al. (US 6,310,966) alone or in combination with other references discloses, teaches, or fairly suggests the claimed invention. The biometric certificates of Dulude et al. includes a validity period data as well as the biometric data information (20) to successfully authenticate a user who wants to access a system or a digital equipment. As discussion shown above, the claims 1-28 are rejected under a new ground of rejection, which are necessitated by the amendment.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Steven S. Paik whose telephone number is 703-308-6190. The examiner can normally be reached on Mon - Fri (7:00am-3:30pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on 703-305-3503. The fax phone numbers for the organization where this application or proceeding is assigned are 703-308-7722 for regular communications and 703-308-7722 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-0530.

Steven Paik
Steven S. Paik
Examiner
Art Unit 2876

ssp
August 14, 2003

MICHAEL G. LEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2800